US DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

Personnel Security/ Suitability Handbook 732.3 Rev 2

Office of Administration

Office of Security and Emergency Planning, Security Division, Personnel Security Branch

9/29/2009

Table of Contents

CHAPTER 1

GENERAL

1-1 Background: This handbook provides the policies and general operating procedures for the administration and operation of the Department of Housing and Urban Development (HUD) Personnel Security and Suitability Program. Its purpose is to ensure that individuals employed by HUD are suitable to perform their duties and responsibilities. These are the controlling instructions for the implementation and maintenance of HUD's personnel security and suitability policies. The handbook serves as a core document to which the Department can look for guidance and that other organizational components can use as a guide to develop their own related handbooks/procedures. The handbook is prepared and updated by the Personnel Security Officer (PSO) in the Office of Security and Emergency Planning (OSEP). Questions, concerns, requests, or suggestions should be directed to the PSO. Changes to the handbook are made on an "as needed" basis.

1-2 Scope: The provisions of this handbook are applicable to all HUD employees and contractors, regardless of position, type of appointment, or tenure. Personnel security and suitability provisions incorporated into other departmental directives must comply with this handbook.

Provisions in this handbook should not have the effect of nullifying or limiting the protections for equal employment opportunity provided in Title VII of the Civil Rights Act, 42 U.S.C. 3535(d), Executive Order (EO) 11478, or HUD's implementation of the 24 CFR Part 7 regulations. HUD will not implement this handbook in such a way as to impede equal employment opportunity on the basis of race, color, religion, sex, sexual orientation, national origin, age, or disability.

1-3 General Provisions of the Personnel Security and Suitability Program:

A. The investigation of all federal and contract employees, with more detailed investigation of incumbents of sensitive positions;

B. The suspension, reassignment, or termination of employees from National Security positions (Critical-Sensitive and Noncritical-Sensitive) when necessary in the interest of National Security; and from public-trust positions (High Risk and Moderate Risk) and Nonsensitive (aka Low Risk) when necessary in the interest of suitability/fitness for the good of the federal service; and

C. Ensuring that due process is provided to an individual who may be removed from a position in the interest of National Security or suitability.

1-4 Legal Authorities:

A. Title 5 U.S.C., Sections 3571, 5596, 7531, and 7532;

B. EO 10450 (Security Requirements for Government Employment); EO 12968 (Access to Classified Information); EO 12958 (Classified National Security Information); and EO 13467 (Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information – guidelines not yet fully implemented); and

C. 5 CFR 731 (Suitability); 5 CFR 732 (National Security Positions); and 5 CFR 736 (Personnel Investigations).

1-5 Roles and Responsibilities:

A. The National Security Council provides overall policy guidance on personnel security and information (classified documents) security.

B. The Office of the Director of National Intelligence (DNI), as the Security Executive Agent, sets the minimum investigative requirements for access to classified information (EOs 12968 and 13467), and is involved in setting standards for safeguarding unclassified sensitive information, including sensitive computer systems, and the issuances or directives that affect intelligence policies and activities.

C. The Information Security Oversight Office of the National Archive and Records Administration is responsible for implementing and monitoring the Classified Information Program established by EO 12958.

D. The Office of Personnel Management (OPM), as the Suitability Executive Agent, is responsible for oversight and implementation of EO 10450 and EO 13467. EO 10450 prescribes security requirements for suitability positions (including investigations) for competitive federal employment. EO 13467 prescribes security requirements (including investigations) for excepted federal employment and contractors.

E. The Federal Bureau of Investigation (FBI) is the chief internal security agency of the federal government with jurisdiction over investigative matters that include, in part, espionage, sabotage, treason, and other subversive activities.

F. The Office of Management and Budget (OMB) represents the President in the development and execution of policies and programs, and has a hand in the resolution of all budget, policy, legislative, regulatory, procurement, e-government, and management issues on behalf of the President.

CHAPTER 2

ACRONYMS, TERMS AND DEFINITIONS

2-1 ACRONYMS

A. Assistant Secretary for Administration—ASA

B. Chief Information Officer—CIO

C. Director of National Intelligence—DNI

D. Department of Defense—DOD

E. Employee Relations Branch—ER

F. Executive Order—EO

G. Executive Personnel Management Division—EPMD

H. General Counsel—GC

I. Government Technical Representative—GTR (aka Contract Oversight Technical Representative—COTR)

J. National Agency Check and Inquiries—NACI

K. Office of the Chief Procurement Officer—OCPO

L. Office of Field Administrative Resources—OFAR

M. Office Human Resources—OHR or HR

N. Office of Information Technology—OIT

O. Official Personnel Folder—OPF

P. Office of Personnel Management—OPM

Q. Office of Security and Emergency Planning—OSEP

R. Personnel Security Branch—PS

S. Personnel Security Officer—PSO

T. Senior Executive Service—SES

U. System Security Administrator—SSA

2-2 TERMS

A. Access

B. Break in Service

C. Classification

D. Contracting Officer

E. Contractor

F. Fitness

G. GTR

H. Information Security Program

I. Initiating an

J. Initiating Request

K. National

L. Nonsensitive

M. Office of Human Resources

N. Position Sensitivity

O. Primary organization

P. Public

Q. Security Clearance

R. Security Violation

S. Sensitive Information

T. Suitability

U. System Owner

V. System Security Administrator

2-3 DEFINITIONS

A. Classified Information – National Security information that has been designated pursuant to the 3 levels as defined in EO 12958, and that is marked "Top Secret," "Secret," or "Confidential."

B. Information Security Program – Deals with the handling and safeguarding of classified information under the guidelines of EO 12968. This program involves primarily the Office of the Secretary (OS), the Office of International Affairs (IA), and the Personnel Security Branch (PS), OSEP. PS has oversight responsibility.

C. National Security Positions – Sensitive positions that involve access to classified information. These positions have OPM-assigned sensitivity codes, and are designated:

1. Special-Sensitive (4)
2. Critical-Sensitive (3)
3. Noncritical-Sensitive (2)

D. Public Trust Positions – Although the public expects all persons working for the

Federal Government to be trustworthy and honest, positions designated as Public Trust are positions that require a higher degree of integrity, with unwavering public confidence in the individual occupying the position. Public Trust positions include, in part, those involving policy-making, major program responsibility, and/or law-enforcement duties. Public Trust positions also are those involving access to or control of unclassified but sensitive information, including significant proprietary or financial records, and those with similar duties through which the incumbent could realize a significant personal gain or cause very serious damage to the public interest. These positions have OPM-assigned sensitivity codes and are designated:

1. High Risk (6)
2. Moderate Risk (5)

E. Primary Organization – Any of the components shown in the Departmental Organizational Chart whose heads report directly to the Secretary or Deputy Secretary.

F. Position Sensitivity – The designated code assigned to a position based on the degree of damage that an incumbent could do to the National Security or federal service.

G. Nonsensitive Positions – Positions that do not afford access to either classified, or other sensitive information, and which are neither National Security nor Public Trust positions.

H. Security Clearance – An administrative determination, based on the appropriate level of background investigation, granting access to national defense classified information, which is "Top Secret," "Secret," or "Confidential," pursuant to the requirements of EO 12968.

I. Office of Human Resources (OHR) – The office that provides administrative personnel functions to the Department in both Headquarters and the Field.

J. Suitability – General fitness or eligibility for career employment with the federal government.

K. Fitness – General fitness or eligibility for excepted or contract employment with the federal government.

L. Break in Service – When employment with the federal government, as either a federal employee or as a contractor, is disrupted for more than 24 consecutive months.

M. Access – The ability or opportunity to gain knowledge of classified or sensitive-but-unclassified information. (An individual may have access to classified or other sensitive information by being in a place where such information is kept if the security measures that are in force do not prevent him or her from gaining knowledge or possession of the information).

N. Security Violation – Any failure to comply with the regulations relative to the protection and security of classified information.

O. Sensitive Information – Any unclassified information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled.

P. Contracting Officer – A federal employee with primary responsibility for one or more contracts.

Q. Government Technical Representative (GTR); aka Contract Oversight Technical Representative (COTR) – A federal employee who provides the technical oversight for a specific contract and directly interfaces with the company's management staff.

R. System Security Administrator (SSA)(aka Program ISSO-Information System Security Officer) – An individual working under the direction of either a

computer system owner, or a manager for the system owner, who ensures that only authorized users have access to HUD's sensitive systems. This person maintains the integrity of the system by:

- Reporting security breaches to the appropriate officials;
- Participating in developing and coordinating system security plans;
- Coordinating and processing user requests for access to the systems;
- Communicating with PS to determine whether a potential system user has undergone the currently-required investigation or has furnished the forms for that investigation through another source;
- Communicating and coordinating with the responsible individuals to ensure that potential users submit the appropriate, properly-completed, background investigation forms (primarily via OPM's electronic investigative forms system, eQIP) for those systems to which access beyond "read" has been determined to be either moderate risk or high risk; and
- Performing other related functions.

S. System Owner – An employee who has the overall responsibility for, or owns, one or more computer systems. This person supervises the system SSA and, in conjunction with the SSA and in accordance with OPM guidelines, designates system sensitivity under the oversight of OIT-CIO.

T. Contractor; aka Vendor – A non-federal employee or firm hired to work on a project.

U. Initiating Request for Electronic Investigative Form – Sending an email link to the individual for the appropriate investigative form.

V. Initiating an Investigation – Furnishing an individual's investigative forms package to OPM to conduct the requested investigation.

CHAPTER 3

INVESTIGATIONS AND SENSITIVE POSITIONS

The standards and criteria for sensitive positions are determined for National Security by the DNI and for suitability/fitness by OPM, and are subject to change. The most recent requirements are identified and communicated either orally or in writing by the PSO.

3-1 Types of Investigations (and the basic coverage):

A. National Agency Check (NAC) – Not a complete investigation, but an integral part of all background investigations – conducted by automated checks;

B. National Agency Check and Inquiries (NACI) – This is an NAC plus written inquiries covering specific areas of a person's background during the past 3 to 5 years. (The NACI is the minimum investigation required for all federal employment, including contractors, except when employment is not to exceed 180 days in the aggregate in a nonsensitive position.);

C. National Agency Check, Inquiries, and Credit (NACIC) – An NACI plus an automated credit check. All credit checks cover at least 7 years;

D. Access NACI (ANACI) – An NACIC with local law enforcement checks, basically covering the past 5 years, plus admitted arrests. Conducted by written inquiries, records checks, and interviews of the subject and others. Unanswered record check inquiries are followed up. (This investigation meets the minimum requirements for federal and contract employees to access classified information at the "Confidential" and "Secret" levels.);

E. NAC with Local Agency Checks and Credit Check (NACLC) – This investigation consists of the same scope of coverage as the ANACI, except that it includes written inquiries only to local law enforcement. (This is the initial minimum investigation for Department of Defense (DOD) contractors and active military service members who require a "Confidential" or "Secret" security

clearance. For other agencies, it also serves as the minimum reinvestigation requirement for federal employees and contractors with "Confidential" or "Secret" security clearance, and whose sensitivity designation would be Nonsensitive or Moderate Risk if they did not require access to classified information. It does not meet the minimum investigative requirements for a primary investigation, except as stated for DOD.);

F. Minimum Background Investigation (MBI) – The NAC, a credit check with no follow up of issue items, 5 years coverage by subject interview and 3 to 5 years coverage by written inquiries of specific areas of a person's background. (Inquiries involving substantial areas of activity, that are undeliverable due to inadequate addresses, are followed up on by request from HUD to OPM after the person has furnished HUD with the correct information.) (If conducted on the SF 86, this investigation meets the requirements for federal and contract employees to access classified information at the "Confidential" and "Secret" level.);

G. Limited Background Investigation (LBI) – The NAC, a credit check with follow up when necessary, 5 years coverage by subject interview, 3 years coverage by a combination of personal interviews, records checks, and written inquiries of specific areas of a person's background. (If conducted on the SF 86, this investigation meets the requirements for Federal and contract employees to access classified information at the "Confidential" and "Secret" level.);

H. Background Investigation (BI) – The NAC, a credit check with follow up when necessary, 5 years coverage by subject interview, 3 to 7 years coverage by a combination of personal interviews, records checks, and written inquiries of specific areas of a person's background. (If conducted on the SF 86, this investigation meets the requirements for federal and contract employees to access classified information at the "Confidential" and "Secret" level.)

I. Single-Scope Background Investigation, aka Special Background Investigation (SSBI or SBI) – This investigation includes the BI, and affords additional coverage up to 10 years. It also requires an NAC of current spouse or cohabitant

and an inquiry into the legal status of foreign-born immediate family members. (This is the required investigation for federal and contract employees to access classified information at the "Top Secret" level);

J. SSBI-Periodic Reinvestigation (SSBI-PR, aka SBIPR) – The required update investigation for individuals who have "Top Secret" clearance. It includes subject and personal interviews, records checks, and written inquiries covering specific areas of a person's background since the previous investigation. (It normally is requested from 5 to 7 years after the previous SSBI or SSBI-PR);

K. Periodic Reinvestigation (PRI) – The required update investigation for individuals whose sensitivity designation is Critical-Sensitive, and who require a "Confidential" or "Secret" security clearance instead of "Top Secret," and those whose sensitivity designation without access to classified information would be High Risk. It consists of an NAC, a subject interview, and a combination of written inquires and records checks covering 5 years of specific areas of a person's background. (It normally is requested from 5 to 7 years after the primary investigation.); and

L. PRI-Residence (PRIR) – This is the PRI, with the addition of 3 years residence coverage by personal interview and records checks.

3-2 Categories of Sensitive Positions:

A. In the context of conducting investigations, OPM requires that sensitive positions be designated in 5 categories:

1. Special-Sensitive (4)

2. Critical-Sensitive (3)

3. Noncritical-Sensitive (2)

4. High Risk (6)

5. Moderate Risk (5)

NOTE: An individual may have computer access at any sensitivity level. OPM requires that this be identified by adding a "C" to the numerical designation.

B. The position sensitivity levels are defined as follows:

1. Special-Sensitive (4) – Positions with access to Sensitive Compartmented Information (SCI), which is an additional authorization to Top Secret, whose occupants have the potential for exceptionally grave damage to the National Security. SCI must be authorized by another agency with authority to do so.

2. Critical-Sensitive (3) – Positions with the potential for exceptionally grave damage to the National Security. All of these positions require Top Secret security clearance. The positions so designated at HUD are:

   a. Presidential appointees;

   b. Positions with emergency preparedness duties;

   c. Positions with access to "Secret" or "Confidential" information, if the position would otherwise be designated High Risk; and

   d. The Personnel Security Officer, Personnel Security Specialists, and other Personnel Security employees who access or safeguard employee security files, or attend classified seminars and training;

3. Noncritical-Sensitive (2) – Positions with the potential for moderate to serious damage to the National Security. These positions require access to "Secret" or "Confidential" information without which the designation code would be either Moderate Risk or Nonsensitive.

4. High Risk (6) – Positions that have the potential for exceptionally serious impact, involving duties especially critical to the Department's mission,

with broad scope of policy or program authority. They include:

a. Positions in the Senior Executive Service (SES);

b. Deputy Assistant Secretaries;

c. Independent spokespersons;

d. Nonmanagers with authority for critically-important independent action;

e. Positions with significant involvement with one or more sensitive computer systems (e.g., SSAs, System Owners, etc.) and to which access beyond "read" requires a higher level investigation than the NACI or MBI to help protect the information; and

f. Positions that require the same degree of public trust as any of the above duties.

5. Moderate Risk (5) – Positions that have the potential for moderate to serious impact, involving duties of considerable importance to the agency or program mission, with significant program responsibility and delivery of customer services to the public, such as:

a. Unsupervised assistance in policy development and implementation;

b. Management or nonmanagement positions with authority for independent or semi-independent action; and

c. Positions with moderate to substantial involvement with one or more sensitive computer systems to which access beyond "read" requires a higher level investigation than the NACI.

CHAPTER 4

DEPARTMENTAL AND STAFF RESPONSIBILITIES

4-1 The Assistant Secretary for Administration has overall responsibility for:

A. Administering HUD's Personnel Security and Suitability Program in accordance with the provisions of EOs 10450, 13467, and 12968, and 5 CFR 731, 732, and 736.

B. Collaborating with the General Counsel, or designee, to jointly recommend to the Secretary disposition of a suspension, reassignment, or termination personnel action.

4-2 Principal Staff are responsible for:

Ensuring that their programs are in compliance with the terms and conditions of this handbook.

4-3 The Chief Information Officer is responsible for:

A. Developing computer-systems security policy and related oversight;

B. Making final determinations on systems sensitivity; and

C. Managing the Information Technology Security Program.

4-4 The General Counsel, or designee, is responsible for:

A. Providing advice in connection with any proposed recommendation by the Assistant Secretary for Administration (ASA) to the Secretary to suspend, reassign, or terminate any individual, and for notifying that individual of the charges supporting the action;

B. Considering any statements or affidavits submitted by the suspended, reassigned, or terminated individual; and

C. Collaborating with the ASA, or designee, to jointly recommend to the Secretary, the disposition of a suspension, reassignment, or termination personnel action.

4-5 The Personnel Security Officer (PSO) is responsible for:

A. Developing and making recommendations concerning Personnel and Information Security Programs, policies, standards, and procedures;

B. Ensuring that every HUD employee and every contractor working on behalf of HUD has on record no less than a NACI; and that the following are investigated to the level required by OPM and DNI:

- occupants of positions designated as sensitive by the Staffing and Classification Division, HR;
- owners of computer systems designated as sensitive and concurred upon by OIT-CIO as sensitive; and
- those determined by the PSO to be sensitive due to access to classified information and other unique duties.

(Investigative requirements are subject to changes, which are communicated by the PSO, either orally or in writing. The current guide for sensitive computer systems is at Appendix A.);

C. Initiating all background investigations above the NACI level for HUD employees and contractors, for whom the responsible parties in HR, the GTR, or SSA, have not verified from a review of the OPF or the SF-75 or from other valid sources that such investigations have been satisfactorily completed and adjudicated. (Currently, the PSO also has the responsibility for initiating all Headquarters NACIs.) (The PSO does not initiate the eQIP request for the investigative forms, except for certain update investigations.);

D. Conducting preappointment/preassignment name checks for the Immediate Office of the Secretary and the Executive Personnel Management Division, HR, on candidates for SES, Schedule C, and Consultant/Expert positions, and for miscellaneous positions as the need arises;

E. Reviewing and evaluating the results of all background investigations, making routine suitability determinations, and signing the Report of Agency Adjudicative Action on OPM Personnel Investigations (INV 79A) to return to OPM on all cases except nonissue NACIs, and signing the Certification of Investigation (COI) to record the investigation in the federal employees' OPFs;

F. Summarizing significant adverse information from reports of background investigations, referring to management through the Employee Relations Branch in Headquarters or the appropriate Field HR office for information or a suitability determination; and after management's closing action, signing the INV 79A and COI (as in 4-5 E. above);

G. Issuing required security clearances, "Top Secret," "Secret," or "Confidential"; obtaining the SF 312, Security Clearance Nondisclosure Agreement for 50-year retention; terminating security clearances when the need no longer exists (and, in both instances, documenting the action for inclusion in the federal employee's OPF and security file, and notifying the employee in writing of the actions taken). (NOTE: Separation from HUD employment automatically terminates a person's security clearance.);

H. Requiring the subjects to furnish their arrest dispositions, or contacting various courts directly for disposition of charges on preappointment or post-appointment arrest records furnished by the FBI through OPM; and either adjudicating the results or furnishing pertinent results to ER in HQ or the Field HR, or direct to management for their information or for a determination of continued suitability/fitness for duty;

I. Providing consultation, advice, and oral or written instructions or guidance relating to HUD's personnel and document security requirements and procedures, including the HUD Personnel Security/Suitability Handbook and National Security Information Handbook, to ensure that the basic responsibilities of EOs 10450, 12968, and 13467, and of 5 CFR 731, 732, and 736 are being met;

J. Establishing, maintaining, and safeguarding personnel security files or records, as appropriate, for all current employees and contractors;

K. Establishing internal operating procedures in accordance with OPM policy and 5 CFR 736 for handling and safeguarding reports of investigation to protect the interests of the individual and HUD;

L. Logging all classified documents received by HUD; conducting required annual inspections of the offices that receive Top Secret classified documents; ensuring that the document custodians have the combination to their document safe changed by a person with the appropriate security clearance at least annually, whenever anyone with the combination leaves, or when there is knowledge or suspicion that the combination has been compromised; ensuring that a document inventory is provided by the document custodian annually; and verifying that a document destruction certificate is executed properly and is furnished by the custodian whenever documents are destroyed;

M. Reconciling, as needed but at least quarterly, the index system database with the listing, furnished by OIT-CIO, of users who require above query access to designated sensitive systems; and

N. Ensuring that background investigations are updated for HUD employees and contractors in Critical-Sensitive and High Risk positions, in accordance with current DNI and OPM guidelines. (Instructions covering updating High Risk are not yet fully implemented by OPM.);

4-6 Office of Human of Resources (OHR)

A. Assisting applicants, employees, and supervisors in understanding and/or preparing any required personnel forms and investigative questionnaires;

B. Ensuring that all applicants for federal positions are fingerprinted via the Personal Identity Verification (PIV) process, and that any required investigative forms are furnished to the appropriate office, to satisfy the requirements of Homeland

Security Presidential Directive 12 (HSPD-12)and EO 10450 (EO 13467 is not fully implemented.);

C. Ensuring that the appropriate background investigation forms are obtained from individuals electronically (with rare exceptions), using OPM's eQIP system, according to OPM/OMB requirements, and ensuring that the questionnaire and required attachments and properly completed and furnished in time for OPM to commence the investigation within 14 working days of the person's entrance-on-duty date. (Currently, Headquarters HR furnishes all investigative forms packages to PS; Field offices submit forms for the NACI directly to OPM for initiation of the investigation; and furnish the SF 85P package to the requesting office – to be forwarded to the appropriate SSA when the person needs sensitive access to a sensitive computer system. The SSA then furnishes those forms to PS.);

D. Ensuring that vacancy announcements reflect appropriate sensitivity levels and that appointment is subject to postappointment investigation and favorable adjudication;

E. Issuing OF-306, Declaration for Federal Employment, to job finalists who have met all qualifications requirements;

F. Referring to OPM's Federal Investigations Processing Center, for a suitability determination or advisory, any competitive applicant situation when evidence of intentional false statement, deception, or fraud in the examination or appointment process is identified on the OF-306;

G. Referring unfavorable information identified on the OF 306 or the SF 75 to ER in Headquarters or the Field, and/or OGC legal counsel for suitability determination or advisory and coordination of actions with the pertinent supervisor, as necessary;

H. Ensuring that all pertinent personnel actions are documented and modified to

reflect appropriate sensitivity levels and that the SF-50-B, Notification of Personnel Action, contains a statement that the action is subject to investigation and favorable adjudication;

I. Ensuring that the automated personnel system contains properly documented position sensitivity codes for positions;

J. Ensuring that the decision to reemploy a person who resigned from another federal agency is based upon complete and pertinent personnel security information; and

K. Notifying PS of employee accessions, separations, name changes, and re-assignments on a biweekly basis.

4-7 The Staffing and Classification Division, HR, is responsible for:

Designation of position sensitivity, according to OPM guidelines, of all positions. (Some positions have automatic sensitivity designations due to established criteria – e.g., SES, persons who require access to classified information, System Owners of one or more sensitive computer systems.)

4-8 The Personnel Benefits and Retirement Center, HR, is responsible for:

A. Ensuring that the COI notice and memoranda issuing security clearances, if required, are included in the OPF;

B. Furnishing eOPFs for PS staff review, when required; and

C. Furnishing eOPFs for OPM and other investigative agencies' review, upon request.

4-9 The Executive Personnel Management Division (EPMD), HR, is responsible for:

A. Furnishing identifying information to PS for a preappointment/preassignment name check on all SES, Deputy Assistant Secretary, Schedule C, Regional Director, Area Office Director, Consultant/Expert positions, and other persons

in the IOS as identified by the AO, IOS. The information includes:

1) Name
2) Social Security Number
3) Date of Birth
4) Place of Birth
5) Position Title and Grade
6) Type of Position
7) Office

B. Furnishing to PS either the SF 86 or SF 85P (via eQIP), as appropriate, and other required investigative forms, in whatever method is standard, unless the person already underwent the needed investigation, and providing the Entrance-on-Duty memorandum.

4-10 The Employee Relations Branch (ER), HR, in HQ and the Field, is responsible for:

Providing advice and assistance to management concerning appropriate action to be taken in relation to actionable adverse suitability/fitness information furnished as a result of a background investigation.

4-11 System Security Administrators are responsible for:

A. Referring initial determinations on system sensitivity to the CIO;

B. Conducting recertification of all systems users' access at least annually, or as defined by the system owners;

C. Identifying positions with duties and responsibilities that require the incumbents to undergo background investigations above the NACI level (See Appendix A);

D. Ensuring that appropriate investigative requirements for each position that entails access to a sensitive system above query access is met (either that the person has undergone the required investigation or has furnished the forms for it,

as in E, below) before enabling a person's access to a sensitive system;

E. Collecting (through established proper channels) and furnishing to PS the required investigative forms containing complete and current information, and a notation that the person has been fingerprinted through the PIV process, for HUD employees and contractors who require above-query access to a sensitive system, and furnishing those investigative forms (primarily via eQIP) and the rest of the package in hard copy under a cover sheet, identifying the person's sensitivity level and the system to which the person is being given access. (This also justifies the investigation above the NACI level.);

F. Referring adverse information on HUD employees to PS for a suitability determination or advisory and coordination with Headquarters or Field ER, and/ or OGC legal counsel;

G. Referring adverse information on contractors to the GTR or Contracting Officer for a suitability determination or advisory and coordination with OGC legal counsel;

H. Notifying the OIT-CIO when access should be denied to a person who requires user access above query to a sensitive system, and:

1) Who has failed to submit properly-completed investigative forms necessary for his/her investigation to be conducted

2) Who has failed to obtain recertification for user access to a sensitive system above query

3) Who has committed any breach of conduct for which access should be suspended or denied, or

4) For whom employment has ended; and

I. Collecting, from the GTR, the date and type of investigation, and the conducting agency, concerning a previous background investigation (without a

subsequent break in federal or federal contract service exceeding 2 years) of contractors, and furnishing that information to PS for verification; and

J. Notifying PS when a person no longer has sensitive access to a sensitive system, including advising when a contractor has separated.

4-12 Government Technical Representatives (aka Contract Oversight Technical Representatives) are responsible for:

A. Collecting appropriate, properly-completed, investigative forms (via eQIP) from contractors; and ensuring that the properly-completed investigative forms for sensitive access are furnished to the SSAs (with the SSA's approval, the GTR may furnish the investigative forms direct to PS on behalf of the SSA, as the SSA's agent) and that the ones for nonsensitive access are furnished to whichever office in HUD initiates the NACIs (currently PS for Headquarters, and ER or OFAR in the Field);

B. Ensuring that the contractor staff establishes personnel security procedures that meet, as a minimum, the requirements of this handbook. The contractor staff shall provide a copy of such procedures, and any revisions made during the period of the contract, to the GTR;

C. Collecting certifications from contractor staff who require access to sensitive systems above query and forwarding them through SSAs to OIT so that access can be granted;

D. Notifying SSAs when continued access should be denied for contractors who have failed to obtain recertification for above-query access to a sensitive system;

E. Ensuring that contractors comply with the personnel security and suitability/ fitness requirements of this handbook; and

F. Notifying SSAs when a contract terminates; when contractors separate; or

when a contractor, for any other reason, no longer needs access to sensitive systems.

4-13 The Office of Information Technology, CIO is responsible for:

A. Coordinating with System Owners, and overseeing and approving, at least annually, the sensitivity designation of the computer systems;

B. Participating with the SSAs in granting access to computer systems; and suspending or terminating, as appropriate, access of individuals who fail to submit properly-completed investigative forms in a timely manner, or who are found to be unfit for continued employment or no longer need access;

C. In conjunction with SSAs, identifying individuals who require background investigations based on their access to sensitive systems; and furnishing appropriate information, either through the SSA or directly to PS for verification of investigations that prospective users claim have been completed and they have had no subsequent break in service exceeding 2 years (see Appendix A);

D. Within 3 working days following the end of each fiscal quarter, OIT-CIO is responsible for providing PS with a quarterly list, in a compatible electronic format containing the name, SSN, name of system, and access level of all individuals who require sensitive access to sensitive systems; and

E. Periodically reviewing all access rights to determine if access is still required.

4-14 Supervisors/Managers are responsible for:

A. Consulting with the appropriate HQ or Field OHR or PS as to the minimum public trust designation and with PS as to the minimum investigation required, when initiating a personnel action for a vacant position;

B. Ensuring that employees promptly submit any required investigative forms (properly completed), SF 85 or SF 85P, via eQIP, to the HQ or Field HR, or the SSA, as appropriate;

C. Promptly providing to the HQ or Field HR, the PS, or the SSA, any acquired unfavorable information regarding the conduct or behavior of an employee or contractor that raises possible suitability/fitness or National Security concerns; and

D. Ensuring that positions under their purview are designated at the proper sensitivity level and informing the HQ or Field HR and SSAs of sensitive systems when there has been a change in duties that could change the position sensitivity designation.

4-17 Employees are responsible for:

Accurately completing, as appropriate, SF 85, SF 85P, or SF 86, via eQIP, as well as other investigative forms, and for submitting them to the requesting HQ or Field HR or other HR office within two working days of their entrance on duty date, or by such pre-appointment date as identified by the requesting office, or of the date of their reassignment to a sensitive position.

4-18 Contractors (aka contract companies), are responsible for:

A. Developing personnel security/suitability (fitness) policies and procedures that comply with OPM regulations and that meet the requirements of this handbook. The contractor staff shall provide a copy of such procedures, and any revisions made during the period of the contract, to the GTR;

B. Providing, in writing, background investigation information to GTRs, when required investigations have been conducted on contractor staff who require access to both sensitive and nonsensitive systems. The notification shall include the following:

- Last Name
- First Name
- Middle Name

- Entire SSN
- Date of Birth
- Place of Birth
- Type of Investigation
- Date of Investigation
- Agency that Conducted Investigation

C. Obtaining appropriate background investigative forms (via eQIP), as well as other forms as identified, from their employees who have not undergone the required investigation; and

D. Notifying GTRs when there no longer is a need for contractor staff to access HUD's computer systems.

4-17 Office of the Chief Procurement Officer is responsible for:

Ensuring that HUD contracts require contract companies to provide either:

1) Verifiable information that their employees who are to be assigned to work on a HUD contract have undergone the needed investigation without a subsequent break in federal or federal contract service exceeding two years, or

2) Appropriate, properly-completed investigative forms (via eQIP) for the level of the background investigation required for the employees' duties.

CHAPTER 5

STANDARDS AND CRITERIA FOR SENSITIVE POSITIONS

5-1 Criteria for National Security and Public Trust Positions – Some criteria for National Security and Public Trust Positions overlap. An individual, found unsuitable for either a National Security or Public Trust Position may be found suitable to occupy a non sensitive position or may be found unsuitable for any federal job and be barred from employment for up to 3 years.

5-2 Standards for Sensitive Positions – The security standard for employment or retention of an individual in a sensitive position is that it is clearly consistent with the interests of National Security or promotes the efficiency of the federal service.

5-3 Criteria for National Security Positions – EO 10450 provides guidelines to determine whether an individual's employment or retention in the federal service is clearly consistent with the interests of National Security. Disqualifying factors shall relate to, but not be limited to, the following:

A. Behavior, activities, or associations that tend to show that the individual is not reliable or trustworthy;

B. Deliberate misrepresentation, falsification, or omission of material facts;

C. Criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, habitual use of intoxicants to excess, drug addiction, or sexual perversion;

D. Illness, including any mental condition, of a nature that in the opinion of competent medical authority may cause significant defect in the judgment or reliability of the employee, with due regard to the transient or continuing effect of the illness and the medical findings in such case;

E. Facts that furnish reason to believe that the individual may be subjected to coercion, influence, or pressure that may cause him/her to act contrary to the best interests of National Security;

F. Commission of any act of sabotage, espionage, treason, or sedition – or attempts, threat, or preparation therefor , or conspiring with or aiding or abetting another person to commit or attempt to commit any such act;

G. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, or with an espionage or other secret agent or representative of a foreign nation whose interests may be inimical to the interests of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States, or the alteration of the form of Government of the United States by unconstitutional means;

H. Advocacy of the use of force or violence to overthrow the government of the United States, or of the alteration of the form of Government of the United States by unconstitutional means;

I. Knowing membership, with specific intent of furthering the aims of, or adherence to and active participation in, any foreign or domestic organization, association, movement, group, or combination of persons that unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or subdivision thereof, or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means;

J. Intentional, unauthorized disclosure, to any person, of security information, or of other information prohibited by law to be disclosed, or willful violation or disregard of security regulations;

K. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States; and

L. Refusal by the individual, on the grounds of constitutional privilege against self-incrimination, to testify before a Congressional committee regarding charges of alleged disloyalty or other misconduct.

5-4 Criteria for Public Trust Positions – 5 CFR 731 provides general guidelines for determining whether an individual's employment, or continued employment, including contractors, will promote the efficiency of the federal service. The general guidelines are as follows:

A. The determination shall be made on the basis of:

1. Whether the individual's conduct may reasonably be expected to interfere with, or prevent, efficient service in the position or effective accomplishment by HUD of its duties or responsibilities; or

2. Whether a statutory or regulatory bar prevents the lawful employment of the individual in the position.

B. When making a determination under this section, any of the following reasons may be considered a basis for finding an individual unsuitable:

1. Misconduct or negligence in prior employment that would have a bearing on efficient service in the position or would interfere with or prevent effective accomplishment by HUD of its duties or responsibilities;

2. Criminal or dishonest conduct related to the person's duties or service in the position, or to other employees' services;

3. Intentional false statement, deception, or fraud in the examination or appointment process;

4. Refusal by a federal employee to furnish testimony in regard to matters inquired of under the civil service laws, rules, and regulations;

5. Alcohol abuse of a nature and duration without evidence of rehabilitation that suggests that the individual would be prevented from performing the position's duties, or would constitute a direct threat to the property or safety of others;

6. Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;

7. Knowing and willful engagement in acts or activities designed to overthrow the Government of the United States by force; and/or

8. Any statutory or regulatory bar that prevents the lawful employment of the person to the position.

C. OPM and other federal agencies shall consider the following additional factors to the extent that they deem these factors pertinent to the case:

1. The kind of position to be filled by the individual, including the degree of public trust or risk in the position;

2. The nature and seriousness of the conduct;

3. The circumstances surrounding the conduct;

4. The recency of the conduct;

5. The person's age at the time of the conduct;

6. Contributing societal conditions; and

7. The absence or presence of rehabilitation or efforts toward rehabilitation.

CHAPTER 6

REQUIREMENTS FOR INVESTIGATIONS AND REINVESTIGATIONS

6-1 Position Designation Requirements – The following apply when an individual has not undergone the required investigation:

A. Special Sensitive and Critical Sensitive Designations – Positions classified in this category are held to the following guidelines:

1. A preassignment investigation, which may not be waived, is required for Special Sensitive positions;

2. A preassignment investigation, or preassignment records checks in conjunction with a post appointment/post assignment investigation, that must be initiated within 14 working days of appointment or reassignment to a Critical-Sensitive position; and

3. An update investigation required every 5 to 7 years for both Special-Sensitive and Critical-Sensitive positions. (OMB has determined a 5 to 7 year time frame for updating.)

B. High Risk Designations – Positions classified in this category are held to the following guidelines:

1. Preappointment/preassignment name checks are conducted on selected positions, primarily those processed by the EPMD;

2. A post appointment/post assignment background investigation must be initiated within 14 working days of entrance on duty or reassignment; and

3. An update investigation is required every 5 to 7 years. (The guidelines covering updating High Risk positions have not yet been fully implemented.)

C. Noncritical Sensitive and Moderate Risk Designations – A post assignment background investigation must be initiated within 14 working days of entrance on duty or reassignment.

D. Nonsensitive Designations – A post appointment NACI must be initiated within 14 working days of the appointment.

6-2 Preappointment and Preassignment Requirements for Certain Positions – HUD has developed preassignment screening procedures for all SES, Deputy Assistant Secretary, Schedule "C," and Consultant/Expert positions. EPMD or the AO, IOS, provides identifying data to PS, which then conducts appropriate name checks and either notifies EPMD of the person's eligibility to occupy the position or furnishes a summary of pertinent information to the AO, IOS for a suitability determination. EPMD notifies PS of the effective date of the individual's entrance on duty and furnishes (via eQIP) investigative forms, if needed, or notifies PS that the person was not selected.

CHAPTER 7

ACTION ON INVESTIGATIVE REPORTS

7-1 Action within HUD – Investigations received from OPM as a result of either an initial investigation or a reinvestigation for anyone who requires a security clearance shall be reviewed and evaluated, as to security and suitability aspects, by PS within 30 days of receipt. Access to classified information may be denied during this period. Initial investigations on persons in all other positions shall be reviewed and evaluated as to suitability/fitness aspects within 90 days of receipt. Representatives of PS may interview or question the employee by written interrogatory to clarify information contained in the investigative data or any other matters related thereto, and may make further inquiries as necessary. The individual shall be fully informed of and given an opportunity to explain or refute derogatory information developed in an investigation before being suspended, reassigned, non-selected, or removed on security or suitability grounds.

7-2 Action Outside HUD – Reports of investigation not completed for HUD, and that were conducted by the FBI or other agencies with investigative authority, do not have a timed closing or reporting requirement, but are processed the same as OPM investigations.

CHAPTER 8

DENIAL OR REVOCATION OF ACCESS TO CLASSIFIED INFORMATION

8-1 Failure to Meet Standards – Applicants and employees, who it is determined do not meet the standards for access to classified information established in section 3.1 of EO 12968, shall be provided with the following, as set forth in the EO:

A. As comprehensive and detailed a written explanation of the basis for that conclusion as the National Security interests of the United States and other applicable law permit;

B. Within 30 days, upon request, and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (3 U.S.C. 552a), as applicable, any documents, records, and reports upon which a denial or revocation is based;

C. Information concerning their right to be represented by counsel or other person at their own expense; the opportunity to request any documents, records, and reports as described in paragraph B above, upon which a denial or revocation is based; and to request the entire investigative file, as permitted by National Security interests and other applicable law, which, if requested, shall be promptly provided prior to the time set for a written reply. (NOTE: The reports of a background investigation can be released only by the FOIA/PA office of the investigating agency.);

D. A reasonable opportunity to reply in writing to, and an opportunity to request a review of, the determination;

E. Written notice of, and reasons for, the results of the review, the identity of the deciding authority, and written notice of the right to appeal;

F. An opportunity to appeal in writing to a high-level panel appointed by the Secretary, which shall be comprised of at least 3 members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in

writing, and are final, except as provided in paragraph 8-2, below; and

G. At some point in the process, an opportunity to appear personally and to present relevant documents, materials, and information before an adjudicative or other authority, other than the investigating entity, as determined by the Secretary. A written summary of such appearance shall be made part of the applicant's or employee's security record.

8-2 Secretary's Authority – Nothing in this chapter shall prohibit the Secretary from personally exercising the appeal authority in 8-1 F., above, based upon recommendations from an appeals panel. In such case, the decision of the Secretary shall be final.

8-3 Suspension of Access – While the procedures described in paragraph 8-1, above, are in process, the PSO will suspend the employee's access to classified information.

8-4 Chief, Employee Relations (ER) Branch – When an employee's access to classified information is suspended, denied, or terminated, the PSO shall inform the Chief, ER, in Headquarters. The Chief, ER, is responsible for the following:

A. Providing advice and assistance to Departmental management officials concerning appropriate action in relation to the individual's employment with the Department. Such advice shall ensure that an individual whose access to classified information has been suspended, denied, or terminated does not perform sensitive duties;

B. Coordinating with appropriate Field ER staff in the cases of employees who are duty-stationed in field offices;

C. Consulting with the Associate General Counsel for Human Resources in Headquarters about the legal sufficiency of any proposed adverse action taken on the basis of suspension, denial, or termination of an employee's access to classified information; and,

D. Obtaining the concurrence of the Deputy Secretary on proposed actions based upon denial or termination of access to classified information when such action is a reassignment to a nonsensitive position or upon the withholding of sensitive duties in the employee's existing position.

CHAPTER 9

REEMPLOYMENT OF INDIVIDUALS WHOSE EMPLOYMENT HAS BEEN TERMINATED

9-1 Reemployment Notification—When it is proposed that an individual who was terminated under the authorities listed in paragraph 1-4 be rehired, the selecting official, or designee shall immediately notify both the Chief, ER, and the PSO, to that effect.

9-2 Restoration within HUD—Any individual whose employment is suspended or terminated under 5 U.S.C. 7532, maybe reinstated or restored to duty under 5 U.S.C. 3571 at the discretion of the Secretary. If reinstated or restored, the individual shall be allowed pay, as provided by 5 U.S.C. 5596.

9-3 Eligibility for Reemployment in Another Agency:

A. Consultation with OPM—Termination under 5 U.S.C. 7532 and EO 10450 does not prevent the person from being employed by any other federal agency. The head of the employing agency, however, must get the approval of OPM for he appointment;

B. Employee requests for OPM Determination—Any civilian employee who is terminated, or resigns while charges are pending under 5 U.S.C. 7532, or any other law or EO authorizing termination in the interests of National Security may request OPM in writing to determine whether he or she is eligible for employment in another agency of the federal government; and

C. OPM Action—OPM will determine and notify the former employee whether he or she may be employed by other federal agencies. OPM also may:

1. Cancel the individual's reinstatement eligibility if it resulted from his or her last federal employment and was obtained through fraud; or

2. Prescribe a period of debarment from the competitive service, not to exceed 3 years. However, these actions may be taken only after a former federal employee found unsuitable under this subsection has had the

opportunity to respond orally or in writing to the reasons for the firing.

Appendix A

Matrix for Background Investigations for Sensitive Computer Systems and Applications

HUD or Contract Staff

Investigation*	Read Only Access	Data Entry	Engineers	Developers and others who change code	Project Leader, Contracting Officer, or GTR	Supervisor of Moderate Risk Positions	System Owner/ System Security Administrator	System Administrator (Hardware) Security Administrator—Contractor (Platform)
Non-Sensitive (NACI)	X							
Moderate Risk (MBI) (Some may warrant LBI)		X	X	X	X	X		
High Risk (BI)				X			X	X

* The types of Investigations listed are guidelines only. They are subject to change pursuant to Office of Personnel Management policy. Final determination as to the type of investigation to be conducted falls within the jurisdiction of the Personnel Security Officer.